



IRS Nationwide  
**TaxForum**

| 2019

*Tax Security 2.0*

*The Taxes-Security-Together Checklist*



IRS

Tax  
Forum

IRS Nationwide

2019

# Seminar Objectives

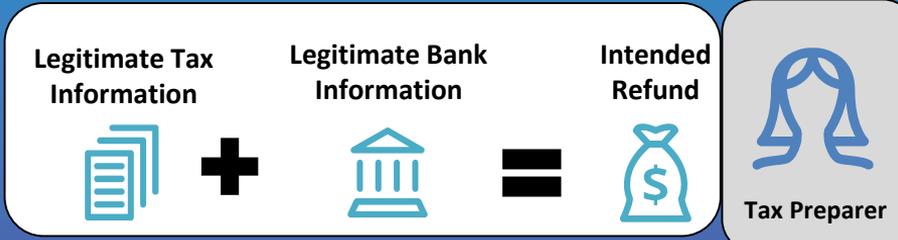
- Review common tax schemes impacting tax professionals
- Review the Taxes Security Together Checklist and the associated Security Six measures.

## Common Schemes

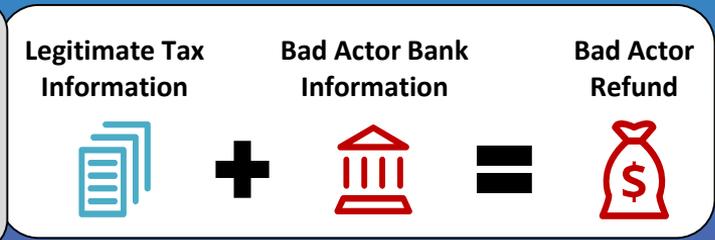
Common schemes that bad actors use to take over preparer accounts include:

- Accessing preparer systems while preparers are connected remotely
- Phishing for preparer account passwords via email
- Hacking into preparer Wi-Fi that isn't password-protected
- Exploiting a lack of firewall and/or anti-virus

### Refund Delivered to Taxpayer



### Refund Delivered to Bad Actor





Tax

Forum

2019

IRS Nationwide

# Taxes-Security-Together Checklist

## ✓ “Security Six” measures

- Anti-virus software
- Firewall
- Two-factor authentication
- Back-up files
- Drive Encryption
- Virtual Private Network





IRS

Tax

Forum

IRS Nationwide

2019

# Taxes-Security-Together Checklist

## ✓ Create a data security plan

- Designate someone to coordinate a plan
- Identify and assess the risks
- Design and implement a safeguards program
- Select service providers that can maintain appropriate safeguards
- Evaluate and adjust the program as necessary

# Taxes-Security-Together Checklist

- ✓ Educate all staff about phishing emails
  - Use separate personal and business email accounts
  - Install an anti-phishing tool bar to ID known sites
  - Use security software, scan emails for viruses
  - Never open attachments from unknown senders
  - Send only password-protected and encrypted documents
  - Do not respond to suspicious or unknown emails
  - Forward IRS-related to [phishing@irs.gov](mailto:phishing@irs.gov)



IRS

Tax

Forum

IRS Nationwide

|

2019

# Taxes-Security-Together Checklist

## ✓ Signs of data theft

- Clients e-filed returns reject because of duplicate SSN
- Clients who haven't filed tax returns begin to receive taxpayer authentication letters (5071C, 4883C, 5747C) from the IRS
- Clients receive unrequested refunds or tax transcripts
- Clients who created an IRS online services account receive an IRS notice that their account was accessed or IRS emails stating their account has been disabled
- Clients unexpectedly receive an IRS notice that an IRS online account was created in their names





Tax

Forum

2019

IRS Nationwide

# Taxes-Security-Together Checklist

## ✓ Signs of data theft

- The number of returns filed with the tax professional's Electronic Filing Identification Number (EFIN) exceeds the number of clients
- Tax professionals or clients responding to emails that the firm did not send
- Network computers running slower than normal;
- Computer cursors moving or changing numbers without touching the keyboard
- Network computers locking out employees

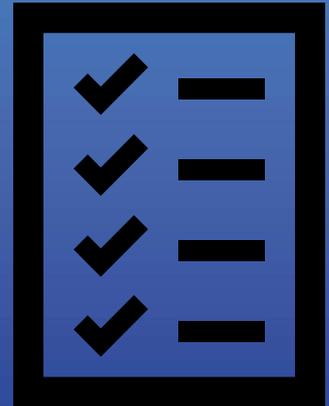


# Taxes-Security-Together Checklist

- ✓ Create a Data Theft Plan/Contact IRS
  - Contact your IRS stakeholder liaison and the IRS data loss mailbox
  - Notify your state tax agency/AG
  - Notify cyber experts/insurance company
  - Review Federal Trade Commission resources

# Taxes-Security-Together Checklist

- ✓ Enact “Security Six” Measures
- ✓ Create a Data Security Plan
- ✓ Educate Staff on Phishing
- ✓ Know the Data Theft Signs
- ✓ Plan, Report Data Losses



Tax  
Forum

IRS Nationwide

2019



## Help and Resources

- ❖ IRS Publication 4557
- ❖ IRS Publication 5293
- ❖ [IRS.gov/identitytheft](https://www.irs.gov/identitytheft)
- ❖ [IRS.gov/protectyourclients](https://www.irs.gov/protectyourclients)
- ❖ FTC's [www.identitytheft.gov](https://www.identitytheft.gov)